Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 09 mai 2007
N° CERTA-2007-AVI-204

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Plusieurs vulnérabilités dans Microsoft Word

Gestion du document

Référence	CERTA-2007-AVI-204
Titre	Plusieurs vulnérabilités dans Microsoft Word
Date de la première version	09 mai 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS07-024 du 08 mai 2007
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

Exécution de code arbitraire à distance.

2 Systèmes affectés

- Microsoft Word 2000 dans la suite Office 2000 Service Pack 3 ;
- Microsoft Word 2002 dans la suite Office XP Service Pack 3 ;
- Microsoft Word 2003 dans la suite Office 2003 Service Pack 2 ;
- Microsoft Word 2003 Viewer dans la suite Office 2003 Service Pack 2 ;
- Microsoft Office 2004 pour Mac ;
- Microsoft Works Suite 2004 ;
- Microsoft Works Suite 2005 ;
- Microsoft Works Suite 2006.

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans l'application Word de la suite bureautique Microsoft Office. L'exploitation de ces dernières permet d'exécuter du code arbitraire sur le système utilisant une version vulnérable.

4 Description

Plusieurs vulnérabilités ont été identifiées dans l'application Word de la suite bureautique Microsoft Office :

1. l'application ne manipulerait pas correctement les données incluses dans les tableaux (*arrays*). Une personne malveillante pourrait ainsi construire un fichier particulier exploitant cette vulnérabilité, afin d'exécuter du code arbitraire sur le système.
2. l'application ne manipulerait pas correctement les objets contenus dans le flux d'un document. L'exploitation de cette vulnérabilité provoque une corruption de la mémoire, permettant ainsi une exécution de code arbitraire. Cette vulnérabilité a fait l'objet de l'alerte CERTA-2007-ALE-006 à la suite d'une diffusion publique de codes malveillants.
3. l'application ne manipulerait pas correctement les propriétés d'un fichier au format `RTF` (ou *Rich Text Format*). L'exploitation de cette vulnérabilité provoque également une corruption de la mémoire, permettant ainsi une exécution de code arbitraire.

5 Solution

Se référer au bulletin de sécurité MS07-024 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Alerte CERTA-2007-ALE-006 du 16 février 2007 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-006/
- Bulletin de sécurité Microsoft MS07-024 du 08 mai 2007 :
  http://www.microsoft.com/france/technet/security/bulletin/MS07-024.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS07-024.mspx
- Référence CVE CVE-2007-0035 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0035
- Référence CVE CVE-2007-0870 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0870
- Référence CVE CVE-2007-1202 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1202

Gestion détaillée du document

09 mai 2007 version initiale.